REMARKS

35 U.S.C § 103

The examiner maintained the rejection of Claims 1-9 and 22-25 under 35 U.S.C. 103(a) as being unpatentable over Cooper US Patent Application Publication 2002/0069200 (hereinafter Cooper), and in view of Symantec's Symantec Antivirus for Macintosh SAM, 1994, (hereinafter Symantec).

The examiner argues that:

> **As per claim 1, Cooper teaches a graphical user interface rendered on a display associated with an intrusion detection system, the graphical user interface comprising: a field that depicts a summary of anomalies identified as part of a event that is detected in a network (throughout the reference, such as Figure 26, paragraph 514, abstract, paragraph 42), the summary indicating event severity details of the event (Figure 26). However, at the time of the invention, Cooper does not explicitly teach an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time. A snooze for future alerts is taught Symantec though, such as in pages 4-9 and 5-6, wherein an event may be allowed to continue, and an alert may be prevented from appearing in the future.**
>
> **At the time of the invention, it would have been obvious to combine the teachings of Cooper with Symantec. One of ordinary skill in the art would have been motivated to perform such an addition, as some anomalies are not necessarily a sign of malicious activity. If this is the case, it would be beneficial to snooze these alerts, as they are not malicious, and it would be more convenient to the user. Symantec teaches in 5-6 that not all suspicious activity alerts necessarily means there is malicious activity.**

Claim 1 requires the features of a graphical user interface including "a field that depicts a summary of anomalies identified as part of an event that is detected in a network, the summary indicating event severity details of the event; and an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time.

The examiner argues that "**Cooper teaches a graphical user interface for an intrusion detection system, the graphical user interface comprising: a field that depicts a summary of anomalies identified as part of a event ....**" Applicant disagrees. Cooper in Fig. 26 for instance depicts a summary listing of various events, which arguably could correspond to Applicant's FIG. 29. However, that is not the claimed limitation of claim 1. Claim 1 calls for: "a field that depicts a summary of anomalies identified as part of an event that is detected in a network." Such a field that depicts the summary of

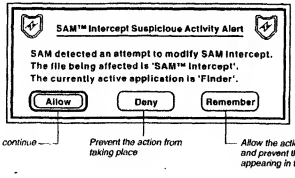
anomalies is depicted in FIG. 30, bottom portion of the pane as "Anomalies detected." The event however itself however is depicted in 312 of FIG. 30 as "Worm propagation suspected." (Subject matter of claim 4).

The examiner also acknowledges that "**Cooper does not explicitly teach an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time.**", and thus relies on Symantec.

Specifically, the examiner argues: "**A snooze for future alerts is taught Symantec though, such as in pages 4-9 and 5-6, wherein an event may be allowed to continue, and an alert may be prevented from appearing in the future.**"

Applicant maintains that Symantec does not suggest any of the features of claim 1. In particular, the feature of "a control to permit a user to snooze future alerts related to the event in the summary for a period of time." Symantec is directed to a virus protection program and not specifically to the claimed intrusion detection in a network. As understood, Symantec product is a machine based product and thus does not operate on network events. The so called snooze feature of Symantec is set forth below:

Figure 4-8



However, the claimed limitation is the feature of "a control to permit a user to snooze future alerts related to the event in the summary for a period of time." Symantec includes an Allow control, that is not a snooze, and a Deny control that is also not a snooze control. Symantec also includes a Remember control. The Remember allows the action to continue, but as stated in Symantec: "Allow the action to continue and prevent this alert from appearing in the future." The Remember control does not meet the features of "a control to permit a user to

snooze future alerts related to the event in the summary. The Remember control also does not operate for a period of time. Thus, because it does not meet either of these two properties of the claimed snooze control, it would not be useful when combined with Cooper, because it could permit what seems like innocuous events to be ignored and erroneously result in a serious network intrusion.

Accordingly, no combination of these references suggests all of the features of claim 1.

Motivation to combine

The examiner also argues that: "**One of ordinary skill in the art would have been motivated to perform such an addition, as some anomalies are not necessarily a sign of malicious activity. If this is the case, it would be beneficial to snooze these alerts, as they are not malicious, and it would be more convenient to the user. Symantec teaches in 5-6 that not all suspicious activity alerts necessarily means there is malicious activity.**" Applicant contends that this motivation is nothing more than an exercise in *ex post* reasoning.

The Supreme Court in *KSR Intl. Co. v. Teleflex Inc.*, 127 S.Ct. 1727 (2007), even while stating that: "the Court of Appeals drew the wrong conclusion from the risk of courts and patent examiners falling prey to hindsight bias," warns that: "a factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning."

> The Court of Appeals, finally, drew the wrong conclusion from the risk of courts and patent examiners falling prey to hindsight bias. A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning. See *Graham*, 383 U. S., at 36 (warning against a "temptation to read into the prior art the teachings of the invention in issue" and instructing courts to "'guard against slipping into the use of hindsight'" (quoting *Monroe Auto Equipment Co. v. Heckethorn Mfg. & Supply Co.*, 332 F. 2d 406, 412 (CA6 1964))). Rigid preventative rules that deny factfinders recourse to common sense, however, are neither necessary under our case law nor consistent with it.

The examiner lays no basis for his conclusion that "**as some anomalies are not necessarily a sign of malicious activity. If this is the case, it would be beneficial to snooze these alerts, as they are not malicious.**" Neither Cooper nor Symantec discloses "a field that depicts a summary of anomalies identified as part of an event" "an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time." Neither Cooper nor Symantec, as pointed out above, lay any basis for snoozing anomalies.

Therefore, the examiner's motivation to combine these references results from *ex post* reasoning, that is, improper hindsight reconstruction, because the examiner could have only gleaned the advantages of the novel combination of claim 1, after reference to Appellant's claims and specification.

In response to Applicants arguments, the examiner makes several points.

As per claim 1, the applicants have amended the preamble to recite that the GUI is rendered on a display associated with an IDS. Amending the preamble does not add to the claim limitations. The display limitation was added to claim 1 to avoid a potential non-statutory subject matter rejection or alternatively, license to ignore claim limitations. Therefore all claim limitations must be considered.

"The applicants also argue that the references teach a virus protection program and not an intrusion detection system. However, again, the intrusion detection system is not claimed, as it is merely in the preamble." Applicant agrees that the previous argument was not particularly helpful. In claim 1, the GUI is for an intrusion detection system and indeed a virus could be considered an intrusion that would be detected by such a system. However the main thrust of that argument was not that it was a virus protection program per se but that it was not networked based.[1]

The examiner also argues that:

> **The applicant also argues that the combination does not teach a snooze function. However, Symantec teaches this by showing the 'remember' function, which allows an action to continue for a certain period of time. These may be later edited in time, if the user actually deems them suspicious or malicious, as taught by Symantec on 5-7, and thus, would be useful with the Cooper combination. Therefore, the combination teaches all the claimed limitations. This would be useful, as stated earlier, as not all suspicious activity alerts necessarily mean there is malicious activity; therefore, it would be advantageous to snooze these alerts to deal with later in case they really are issues.**

The remember function neither permits a user to snooze future alerts related to the event in the summary because neither reference suggests "a field that depicts a summary of anomalies identified as part of an event," nor permits this to occur for a period of time. In Symantec the Remember function can be edited by the user but that does not meet the claim limitation of a

---

[1] Specifically it was argued that:

Symantec is directed to a virus protection program and not specifically to the claimed intrusion detection in a network. As understood, Symantec product is a machine based product and thus does not operate on network events.

period of time because there is no period that can be specified by some feature that needs to be edited by a user in order to resume alerting the user.

Claim 2

Claim 2 requires the feature that "the snooze control feature is selected based on event types and roles of hosts." The examiner in response to Applicant's argument stated:

> **As per claim 2, the applicants argue that Cooper does not teach alerts based on grouping or roles of hosts. However, as cited in the previous office action, security policies based on roles of hosts are taught in Cooper in paragraph 100 and 158.**
>
> **Paragraph 100 teaches wherein policy may be based on communities of hosts, servers, subnets and firewalls, as well as service level. Also, as seen in table A in paragraph 86, communites of hosts are grouped together when they have similar functions/roles.**

Whether or not Cooper's "communities of hosts" correspond to roles of hosts, the examiner's argument that: "**However, as cited in the previous office action, security policies based on roles of hosts are taught in Cooper in paragraph 100 and 158.**" does not follow that Cooper at the cited passages teach alerts based on grouping or roles of hosts. Symantec being directed to a stand-alone application would not be concerned with grouping or roles per se and therefore no combination of Cooper with Symantec would suggest the features of claim 2.

Claim 3 is allowable at least for analogous reasons as in claim 1.

Claim 4

Claim 4 recites that "… an event details region of the graphical user interface depicts anomalies that were used to classify the event." The examiner argues in response that: "**As per claim 4, Cooper does indeed teach that GUIs are used to depict anomalies that were used to classify the event, in Figure 12. The disposition, such as an invalid url, probable scan, are anomalies.**" However, that is not what Applicant argued.[2] Applicant argued that because in Applicant's view Cooper teaches events, and nto did

[2] Applicant argued:

> Claim 4 limits claim 3 requiring that "an event details region of the graphical user interface depicts anomalies that were used to classify the event." The examiner argues that: "**…Cooper teaches wherein an event details region of the graphical user interface depicts anomalies that were used to classify the event (Figure 22).**" Applicant disagrees. Cooper is not understood as dealing with anomalies (e.g., low level network discrepancies that are used to form and classify an event) and events. Therefore Cooper cannot teach that the "interface depicts anomalies that were used to classify the event."

not teach anomalies and events, that: "Therefore Cooper cannot teach that the "interface depicts anomalies that were used to classify the event." If the examiner persists in this interpretation of Cooper, then Applicant request that the examiner specifically point out where Cooper shows the interface that depicts anomalies that were used to classify the event.

The examiner maintained the rejection of Claims 10-14 and 18 under 35 U.S.C. 103(a) as being unpatentable over Cooper and Symantec, as applied above, and further in view of Billhartz US Patent No. 6,986,161 (hereinafter Billhartz).

Claim 10

Claim 10 includes the features of "... providing an operator with a list of events identified by an intrusion detection system, within the list of events being information indicating event severity, with event severity determined for an event, by the event having a percentage relationship to an established threshold for issuing an event notification; displaying details of a selected one of the events to a user; and providing on a graphical user interface a snooze control to allow a user to snooze future alerts related to the selected event.

In addition to the features discussed for claim 1 above, claim 10 includes "with event severity determined for an event, by the event having a percentage relationship to an established threshold for issuing an event notification." Claim 10 is allowable at least for the reasons discussed in claim 1. Moreover, Billhartz is not seen as curing the deficiencies of the combination of references.

The examiner argues that:

> **Independent claim 10 is rejected using the same basis of arguments used to reject claim 1 above. However, Cooper and Symantec do not explicitly teach an event severity having a percentage relationship to an established threshold for issuing an event notification. This is taught throughout Billhartz though, such as in col. 8 line 41 to col. 9 line 10.**
>
> **At the time of the invention, it would have been obvious to one of ordinary skill in the art to include basing event notifications on percent relationships. One of ordinary skill in the art would have been motivated to perform such an addition to provide greater certainty when issuing alerts, thereby reducing false positives. As indicated in col. 2 liens 15-23 of Billhartz, the previous intrusion detections systems do not reliably indicate whether some nodes are rouge or legitimate nodes.**

Billhartz col. 8, line 41 to col. 9, line 10, as understood, discloses determination of a threshold number of collisions of packets to detect intrusions into the network. While Billhartz mentions that: "**the threshold number may be based upon a percentage of a total number of monitored packets having the predetermined packet type ... , then the intrusion alert may be generated,**" the claimed feature is to event severity determined for an event by the event having a percentage relationship to an established threshold for issuing an event notification. Accordingly, Billhartz does not suggest the claimed feature.

Claims 11-14 are allowable for the reasons discussed in claim 10 and for analogous reasons given above. For instance, claim 12 includes analogous features as claim 2, and so forth.

Claim 18

Claim 18 includes the feature of "... displaying event details including destination and source fields populated with IP addresses and role classification of the host in the network."

The examiner argues that:

> **As per claim 18, as best understood by the Examiner, details of source and destination populated with IP addresses is taught throughout Cooper, as can be seen in Figures 23. Cooper then teaches the preventing of unnecessary alerts due to roles of hosts, such as in paragraphs 100 and 158.**

Claim 18 further distinguishes over Cooper taken with Symantec, because, not only does it require displaying event details including destination and source fields populated with IP addresses, it also requires displaying of "role classification of the host in the network." Cooper's alleged teaching of "**Cooper then teaches the preventing of unnecessary alerts due to roles of hosts, such as in paragraphs 100 and 158.**", taken with the alleged teaching of event details including destination and source fields populated with IP addresses, does not suggest all of the features of claim 18.

The examiner rejected claims 15-17 and 21 under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Porras US Patent No. 6,321,338 (hereinafter Porras).

Claims 15-17 and 21 are allowable at least for the reasons discussed in claim 10.

The examiner rejected claim 19 under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Central Point's Central Point Anti-Virus- Virus detection, Removal and Prevention, 1991 (hereinafter Central Point).

Claim 19 is allowable at least for the reasons discussed in claim 10.

The examiner rejected claim 20 under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, as applied above, and further in view of Kuroshita US Patent No. 5,550,807 (hereinafter Kuroshita).

Claims 20 is allowable at least for the reasons discussed in claim 10.

No fee is due. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 5/2/05

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906